

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001524

International filing date: 02 February 2005 (02.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-307953
Filing date: 22 October 2004 (22.10.2004)

Date of receipt at the International Bureau: 24 March 2005 (24.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日本国特許庁 03.2.2005
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2004年10月22日
Date of Application:

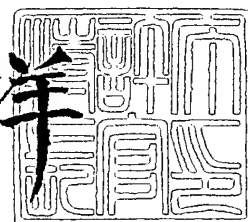
出願番号 特願2004-307953
Application Number:
[ST. 10/C]: [JP2004-307953]

出願人 株式会社サイバー・ソリューションズ
Applicant(s):

2005年 3月10日

特許庁長官
Commissioner,
Japan Patent Office

小川 洋



【書類名】 特許願
【整理番号】 CYBER001B
【あて先】 特許庁長官殿
【国際特許分類】 G06F 13/00
【発明者】
 【住所又は居所】 宮城県仙台市青葉区南吉成 6 - 6 - 3
 【氏名】 キニ グレン マンスフィールド
【特許出願人】
 【識別番号】 501175281
 【氏名又は名称】 株式会社サイバー・ソリューションズ
【代理人】
 【識別番号】 100088096
 【弁理士】
 【氏名又は名称】 福森 久夫
 【電話番号】 03-3261-0690
【先の出願に基づく優先権主張】
 【出願番号】 特願2004- 25015
 【出願日】 平成16年 2月 2日
【先の出願に基づく優先権主張】
 【出願番号】 特願2004-267519
 【出願日】 平成16年 9月14日
【手数料の表示】
 【予納台帳番号】 007467
 【納付金額】 16,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 0306732

【書類名】 特許請求の範囲**【請求項 1】**

インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フィールドの値の数が一定時間内で所定数、若しくは所定率に達した場合には不正攻撃が行われていると判定することを特徴とする不正情報検知システム。

【請求項 2】

前記フィールド値の値の数とパケット数を監視することを特徴とする請求項 1 記載の不正情報検知システム。

【請求項 3】

前期フィールドの値の数と通信量（オクテット数／ビット数）を監視することを特徴とする請求項 1 記載の不正情報検知システム。

【請求項 4】

前記フィールドの値は、複数のフィールドの組合せにより構成されていることを特徴とする請求項 1 又は 2 記載の不正情報検知システム。

【請求項 5】

インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組合せに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする請求項 1 乃至 4 のいずれか 1 項記載の不正情報検知システム。

【請求項 6】

インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組合せに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする不正情報検知システム。

【請求項 7】

インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フィールドの値の数が一定時間内で所定数、若しくは所定率に達した場合には不正攻撃が行われていると判定し、

インターネットの複数個所で前記フィールドの値の数を監視することにより不正な送信元を探索するようにしたことを特徴とする不正攻撃元探索システム。

【請求項 8】

前記フィールドの値は、ヘッダ内の複数のフィールドの個々の組合せにより構成されていることを特徴とする請求項 7 記載の不正攻撃元探索システム。

【請求項 9】

インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組み合わせに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする請求項 8 記載の不正攻撃元探索システム。

【書類名】明細書

【発明の名称】不正情報検知システム及び不正攻撃元探索システム

【技術分野】

【0001】

本発明は、インターネット回線を通じて送信されてきた情報が適正な情報であるかあるいは(D)DoSなどの不正な情報であるかを判定する不正情報検知システム及び不正攻撃元探索システムに関するものである。

【背景技術】

【0002】

【特許文献1】特開2003-318987号公報

【特許文献2】特開2003-234784号公報

【0003】

近年、ある企業や組織をターゲットにし、大量の不正な通信（パケット）を送信するサービス妨害攻撃が問題となっている。このような(D)DoS攻撃は、一般にはサーバの処理能力を超える大量の接続要求を一度に送りつけることや、通信回線の容量を不要な通信で埋め尽くすことで他の必要な通信を妨害し、通常業務を妨害したり、課金制ユーザーに対するプロバイダへのアクセス時間並びに通信会社への通信時間を延長させて納付料金を高騰させるといった弊害を与えるものである。いわゆる(D)DoS攻撃といわれるものである。

【0004】

(D)DoS攻撃とは、攻撃対象機器およびネットワークの処理能力を上回る非常に甚大な数のパケットを送りつけ、対象のサービスを不能にしてしまう攻撃方法である。

【0005】

そこで、各パケットのヘッダ部分に含まれるSourceアドレス（送信元アドレス）を管理し、このような(D)DoS攻撃を送りつけたアドレスからの通信を2度と受信しないと共にその送信元に通信の終了を示すパケットを送り返すといった防止機能を付加したサービスが見受けられる。

【0006】

しかしながら、このような防止サービスは、異なったSourceアドレスから(D)DoS攻撃を送りつけてきた場合には、その(D)DoS攻撃の受信を拒否することができないといった問題が生じていた。

【0007】

一方、このような(D)DoS攻撃を送りつける送信元では、受信拒否された(D)DoS攻撃が送り返されてしまうと、自身のサーバおよびネットワークが容量オーバーとなってしまう。従って、送信元では、Sourceアドレスをランダムに偽造作成し、大量のパケットの各アドレスを異ならせたうえで特定宛先アドレスに(D)DoS攻撃を送信するといった対応で対抗してきているのが実情である。

【0008】

これに対し、例えば、特許文献1では、不特定多数の電子メールに対し、電子メールのデータフォーマットのヘッダ部分に含まれるToアドレス（送信先アドレス）を事前設定されたアカウント別メールヘッダ・コンテンツ書き換え定義にしたがい、受信した電子メールを書き換えた上でその書き換えメールアドレスに再送信（転送）し、特定メールサーバへの負荷を分散させている。

【0009】

また、特許文献2では、同時に送信されてきた電子メールのFromアドレスに不明なものを大量に含むか否かを判定し、Fromアドレスに不明なものが大量に含まれている場合には、その送信されてきた大量の電子メールのFromアドレスに送信メールを返信し、返信できた電子メールのみを適正な電子メールとして受信している。

【発明の開示】

【発明が解決しようとする課題】

【0010】

ところで、送信元アドレスは容易に偽造し変更することが可能であるため、大量の送信元アドレスを事前に予測し、対応することは非常に困難である。

【0011】

また、(D)DoS攻撃は個々のパケットレベルでは正常な通信との区別が困難なことから、なんらかの閾値を用いた検知が検討されているが、それらは対象となるネットワークの特性や利用状況によって大きく変化するものであるため、高い検知精度は期待できない。

【0012】

また、(D)DoS攻撃は正常な通信との識別が困難なことから、間違った判断により正常な通信の送受信をも遮断してしまう可能性があった。

【0013】

このように、従来技術では、(D)DoS攻撃の判定基準が複雑となっているため、検知が困難な小規模の(D)DoS攻撃の受信を余儀なくされたり、必要な通信をも受信拒否してしまうといった問題が生じていた。

【0014】

本発明は、上記問題を解決するため、(D)DoS攻撃などの不正攻撃があるか否かの判定基準を容易に行うことが可能な不正攻撃検知およびその追跡システムを提供することを目的とする。

【課題を解決するための手段】

【0015】

請求項1に係る発明は、インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フィールドの値の数が一定時間内で所定数、若しくは所定率に達した場合には不正攻撃が行われていると判定することを特徴とする不正情報検知システムである。

フィールドの値としては、例えば、次のものが上げられる。

バージョン
ヘッダ長
ToS
全長
アイデンティフィケーション
フラグ
フラグメントオフセット
Time to Live
プロトコル
ヘッダチェックサム
発信元アドレス
到達先アドレス
オプション
ポート

あるフィールドの値の数は、例えば、フィールドの値が「発信元アドレス」として、区別できる発信元アドレスとして、 a_1 (=一郎)、 a_2 (=二郎)、 a_3 (=三郎)、 $\dots a_n$ (=n郎)があった場合、フィールドの値の数は n である。

【0016】

フィールドの値の数が、任意に決めた値の数以上になった場合に不正攻撃が行われていると判断する。任意の決めた値は、例えば、ある時点における数 n_{t1} に比較して他の時点における数 n_{t2} が k 倍以上(k は例えば2以上の数)となったときに不正攻撃が存在すると決めてもよい。なお、フィールドの値の数が減少する場合にも不正攻撃の存在があると判断する場合もある。

【0017】

請求項2に係る発明は、前記あるフィールド値のパケット数を監視することを特徴とする請求項1記載の不正情報検知システム。

【0018】

フィールドの値の数 f_n とともにパケット数 p_m を監視し、その比で判断してもよい。ある時点における比 $(f_n / p_m) t_1$ がある任意に決めた値以上になった場合に不正攻撃が存在すると設定してもよい。 $(f_n / p_m) t_1$ と $(f_n / p_m) t_2$ との比がある値以上になったときに不正攻撃と判断してもよい。

【0019】

請求項3に係る発明は、前記フィールドの値は、複数のフィールドの組合せにより構成されていることを特徴とする請求項1又は2記載の不正情報検知システムである。

【0020】

フィールドの値として「発信元アドレス」と「到達先アドレス」との組合せによりフィールドの値を構成する。

【0021】

まず、前記同様、発信元アドレスとして、 a_1 (=一郎)、 a_2 (=二郎)、 a_3 (=三郎)、 \dots a_n (=n郎) があったとする。

【0022】

a_k ($k=1 \sim n$) について、到達アドレスの種類が m_k 個あるとすると、この場合における複数のフィールドの組合せにより構成されるフィールドの値の数は $\sum m_k$ ($k=1 \sim n$) となる。

【0023】

請求項4に係る発明は、インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組合せに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする請求項1～3のいずれか1項記載の不正情報検知システムである。

【0024】

請求項5に係る発明は、インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組合せに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする不正情報検知システムである。

【0025】

請求項6に係る発明は、インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フィールドの値の数が一定時間内に所定数、若しくは所定率に達した場合には不正攻撃が行われていると判定し、インターネットの複数個所で前記フィールドの値の数を監視することにより不正な送信元を探索するようにしたことを特徴とする不正攻撃元探索システムである。

【0026】

請求項7に係る発明は、前記フィールドの値は、ヘッダ内の複数のフィールドの個々の組合せにより構成されていることを特徴とする請求項6記載の不正攻撃元探索システム。

【0027】

請求項8に係る発明は、インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組み合わせに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする請求項7記載の不正攻撃元探索システムである。

【発明の効果】

【0028】

本発明の不正情報検知システムによれば、同時に大量に送信されてきたパケットに対し、その大量のパケットの値の数又はパケット数が一定時間内に所定数に達した時に、略同期して送信元アドレス件数が所定数若しくは所定率に達した場合には、その大量の電子メールを(D)DoS攻撃メールと判定することにより、特定の送信元アドレスに対して受信許可設定若しくは受信拒否設定をするといった細かく煩わしい設定をすることなく(D)DoS攻撃が送信されてきたことを認識および追跡することができる。

【発明を実施するための最良の形態】**【0029】**

前述した通り、D o S 攻撃とは、攻撃対象機器に処理能力を上回る非常に甚大な数のパケットを送りつけ、対象のサービスを不能にしまう攻撃方法である。

このD o S 攻撃は次のような特徴を有している。

【0030】

例えば、ヘッダ内のフィールドの値の一つである発信元アドレスは偽造されている（偽のアドレスが用いられている）攻撃元の発信元

アドレスであるパケットをフィルタすることにより、D o S 攻撃をブロックされないように、D o S 攻撃の発信元アドレスはランダムに選択されていることが一般的である。

【0031】

D o S は非常に莫大なパケットが送信されるので、次のような方法で検知される。

【0032】

第1の方法は、攻撃パケットもしくは、不正なパケットの数を数える方法である。どのようなパケットが不正であるかを判断することはむずかしい。なぜなら、D o S 攻撃に使われるパケット一つ一つは正常なパケットであるからである。

【0033】

第2の方法は、検知したパケット全て（攻撃パケットも含む）を数える方法である。ネットワークトラフィックは時々刻々動的に変化する。従って、単にネットワークトラフィック量が増大したからといって、その現象はD o S 攻撃によるものと指摘することはできない。また、既にトラフィック量が飽和状態である場合は、D o S 攻撃があったとしても、トラフィック量は増加しない。

【0034】

それに対して、本形態における方法は、D o S 攻撃の検知方法は、トラフィックの発信元アドレスを数える方法である。もし攻撃者がランダムに発信元アドレスを選択しているならば、観測される発信元アドレスの数も増加しているはずである。ある一定時間間隔では、1個の発信元アドレスに対して、そのような発信元アドレスを持つパケットは複数観測されるのが通常である。しかし、攻撃の最中では一般的に1個の（偽造された）発信元アドレスに対して、攻撃パケットは1個しか観測されない。このようにD o S 攻撃を検知することができる。

【0035】

発信元アドレス、到達先アドレスとその他の情報・データから構成されている。時間間隔でパケットを数える。例えば、図3に示すように、ネットワーク（Net1）と攻撃先（Target）との間の経路にパケットを観測するための手段を設けておき、そこで、パケットを観測すればよい。かかる手段としては、例えばスニファ（Sniffer）やパッシブ型プローブなどの機器がある。

【0036】

スニファ（Sniffer）や、パッシブ型プローブなどの機器は全てのパケットを観測でき、それらの機器は以下の値を数えあげることができる。

パケットの全数

ある特定の発信元アドレスを持つパケット数

ある特定の到達先アドレスを持つパケット数

発信元アドレス毎のパケット数

到達先アドレス毎のパケット数

特定のタイプのパケット数

これらの値は、一定時間間隔毎に収集可能である。

【0037】

次にD o s 攻撃の追跡方法について述べる。

【0038】

D o S 攻撃元の追跡方法としては、第1に、不正なパケットの経路をチェックする（パ

ケット追跡) 方法がある。しかし、どのようなパケットが不正なのかを知る必要がある。

【0039】

第2に、トラフィックパターンをチェックする方法がある。しかし、この方法は、不正確である。

【0040】

それに対して、本発明の実施の形態においては、経路上において観測されるアドレス数の変化をチェックする方法である。全ての経路地で同様な現象が観測されると推測される以下のようなパターンが観測される。

【0041】

時間 (任意単位)	パケット数	発信元アドレス数
1	1000	50
2	800	60
3	900	57
4	1200	64
5	50	30
6	1500	530
7	1800	550
8	1700	570
9	800	80
10	900	65

上記において、時間6、7、8においては、パケット数とともに発信元アドレス数が増加している。そこでは、D o S 攻撃がなされている。

【0042】

一方、図4に示すように、インターネットの各経路にスニファース n ($n=1, 2, 3, \dots$) を置いておき、そこでの観測結果同士を比較すればどの経路でD o S 攻撃がなされているかを知ることができる。その経路を遮断すればD o S 攻撃元を追跡することができ、必要に応じてその経路を遮断すればよい。また、その経路からの所定のパケットを遮断すればよい。

【0043】

なお、本発明において、フィールドの値としては、IPv4 プロトコルパケットを例にした場合、次のものが例示される。

バージョン領域
ヘッダ長領域
ToS 領域
全長領域
アイデンティフィケーション領域
フラグ領域
フラグメントオフセット領域
Time to Live 領域
プロトコル領域
ヘッダチェックサム領域
発信元アドレス領域
到達先アドレス領域
オプション領域
ポート領域

【0044】

本発明においては、これらのフィールドの個々の値の件数を検知してもよい。また、これらの個々のフィールドの値の2以上の任意の組合せをフィールドの値としてその件数を検知してもよい。

【0045】

以下に例を示す。

カテゴリは一つ、ないしは複数のヘッダ領域によって定められるパケットを分類できる性質のことである。

(カテゴリの例) プロトコル領域がTCPであるパケット全て

便宜上“Total カテゴリ”というカテゴリを定義する。全てのパケットはこのカテゴリに属する。

【0046】

今までの統計分析手法は、モニタや探査装置により観測されたパケットから、全ての観測パケット数や、あるカテゴリに対するパケット観測数などの標本値を元にしてきた。

【0047】

【表1】

(例) プロトコル領域毎のパケット数

	全体	TCPパケット	UDPパケット	ICMPパケット
10:01	181	123	46	0
10:02	142	100	32	10
10:03	206	140	0	13
10:04	217	120	87	10

Etc...

【0048】

カテゴリ変換 (C-Transform) における統計分析では、検知したパケットが属するカテゴリの数に着目する。上記の例において、プロトコル領域ごとのカテゴリの数を見た場合以下の通りになる。

【表2】

	全体	TCPパケット	UDPパケット	ICMPパケット	カテゴリの数
10:01	181	123	46	0	2
10:02	142	100	32	10	3
10:03	206	140	0	13	2
10:04	217	120	87	10	3

このようにパケットの数の分布からカテゴリの数の分布を作成する方法のことをカテゴリ変換 “C-Transform” と呼ぶ。

【0049】

いくつかのヘッダ領域の和によって作成されたカテゴリがとる事が可能な最大のカテゴリの数はその領域の合わせた幅による。例えば幅が合わせて4ビットの領域で作成される彼ごりの場合、最大のカテゴリの数は16個 (2の4乗) である。

【0050】

しかし、IPヘッダにおけるVersion領域とProtocol領域のように、予め定義された以外の値を持つことができないヘッダ領域がある (ASSIGNED NUMBERS, RFC 790 参照)。そのためこのような領域から作成できる意味のあるカテゴリは限定される。

【0051】

また、32ビット (4294967296) の幅を持つ発信元アドレス、到達先アドレスのように非常に大きな値を取り得る領域からのカテゴリ変換 (C-Transform) は特に興味深い統計を提供することになる。

【0052】

本発明においては、インターネット回線上における、前記情報のカテゴリ数が所定の値となった場合に当該情報を不正情報と認定する。またホップ数を効果的に活用することで検知および追跡の効率を向上する。

【0053】

(検知方法)

カテゴリ数、パケット数、通信量をそれぞれ以下のように定義する。 $1 \dots i$ は時系列に並んだ値とする。

カテゴリ数 : C_1, \dots, C_i, \dots

パケット数 : P_1, \dots, P_i, \dots

通信量 : O_1, \dots, O_i, \dots

このとき、以下の条件で検知する。

a. $C_i > T$

b. $C_i / C_{i+1} > T$

c. $C_i / \{P_i | O_i\} > T$

T は閾値である

T は固定値もしくはトラフィックデータから算出される値である

例えば、 $T = F \times \text{movingAverageOfStatistic (in a, b, c above)}$

のように上記の a, b, c の値の移動平均になんらかの数 F を乗じて差出されたものである。

F は固定あるいはトラフィックデータから算出される値である

例えば、 $F = A \times \text{standardDeviationOfStatistic}$

のように標準偏差を用いて算出されることもある。

A は定数である

インターネットにおいては、情報の無限循環を防止するために、ヘッダの TTL (Time to Live) のフィールドの値に基づき HOP (ホップ) の数が 0 となったらその情報をインターネット上から落とすことが行われている。ところで、ある送信元情報が示された場合、それが詐称されたものではなく正規の場合 HOP 数はほぼ決まっている。したがって、その決まっている HOP 数と比較して、実際に送られた来た詐称情報の場合の HOP 数が異なる場合その情報は不正情報と判断することができる。

【実施例】

【0054】

次に、本発明の(D)DoS攻撃検知およびその追跡システムの実施の形態を図面に基づいて説明する。

【0055】

図1は本発明の(D)DoS攻撃検知およびその追跡システムを示す図である。図1において、1はインターネット回線、2はインターネット回線1に接続された送信元のコンピュータ本体、3はインターネット回線1に接続された受信側コンピュータ、4はインターネット回線1と受信側コ

ンピュータ3との間に接続された通信監視装置である。

【0056】

尚、この通信監視装置4はネットワークに接続されるが、受信側コンピュータ3がサーバー等であった場合には、そのサーバーを通信監視装置4としても良い。

この場合、受信とはサーバーで割り当てたポートに対する通信の受信を意味、判定のための受信は含まないものとする。また、受信側コンピュータ3がプロバイダ所有のメールサーバーであった場合には、他のインターネット回線を通じてメール受信端末(例えば、パーソナルコンピュータ等)が接続されることとなる。

【0057】

通常、送信側コンピュータ2から送信されるパケットは、図2(A)に示すように、その通信を構成するパケットのパケットデータフォーマット10のヘッダ部11に、送信元

アドレスに相当するSourceアドレス 1 2 と送信先アドレス（受信側アドレス）に相当するDestinationアドレス 1 3 とが含まれている。

【0 0 5 8】

通信監視装置 4 は、送信された値の数若しくはパケット数と、Sourceアドレス 1 2 の件数とを監視する。

【0 0 5 9】

例えば、通常の送受信を想定した場合、送信元コンピュータ 2 から受信側コンピュータ 3 に送信される値の数は 1 件であり、例え、他の送信側コンピュータ（図示せず）から略同時期に他の通信が受信側コンピュータ 3 に送信されたとしても、その値の数とSourceアドレス 1 2 とは 1 対 1 で比例して増える。

【0 0 6 0】

また、例えば、特定の通常の通信が偶然大容量となることがあり得る。この場合、従来の通信量に基づく検知では、その量だけを問題として、不正であると誤って判断されることがある。

【0 0 6 1】

この問題は、多くの通信が集まる人気のあるコンテンツを運用するサーバでは特に顕著な問題となり、通常の通信と (D)DoS 攻撃を識別することが非常に困難となる。

【0 0 6 2】

このような場合、メール監視装置 4 では、図 2 (B) のピーク P 1 に示すように、通信量としては通常の通信量よりも多い件数のパケットが送信されてきた判定する。

【0 0 6 3】

しかしながら、各パケットのSourceアドレス 1 2 は共通、あるいは特定のグループで占められることから、そのパケットを正式に受信する。尚、カテゴリ数が所定数以内であった場合（例えば、1 0 件未満）に、その受信を許容するようにしても良い。

【0 0 6 4】

一方、実際には 1 台の送信側コンピュータ 2 から送信されたパケットでありながら、送信元アドレス（Sourceアドレス 1 2）をランダムに偽装して大量のパケットを受信側コンピュータ 3 に送信してきた場合、通信監視装置 4 では、図 2 (B) 及び図 2 (C) のピーク P 2, P 3 に示すように、通信量（若しくはパケット数）が通常の通信の送受信のときよりも多くなると同時に、その各パケットのSourceアドレス 1 2 も略同時期に増大することになる。

【0 0 6 5】

従って、通信量（若しくはパケット数）が所定数（例えば、1 0 0 件）を越えた際、Sourceアドレス 1 2 の数も略同時期に所定数（例えば、9 0 件）若しくは所定率（例えば、パケットの数に対して 9 0 %）を超えた場合には、その受信を拒否する。

【0 0 6 6】

尚、このような一斉同時送信に対応した一定時間内に送信されてきた通信の件数（若しくはパケット数）の所定数並びにSourceアドレス数の所定数の設定は、サーバーの処理能力やネットワークの容量に応じたり、受信側コンピュータ 3 の所有者の業種等に応じたりして設定することができる。

【0 0 6 7】

例えば、受信側コンピュータ 3 の所有者の業種がインターネット検索サービスやチケット販売等であった場合、多くの人の検索要求や人気のある旅行プランやイベント内容に対するアクセスが殺到するといったことが想定される。

【0 0 6 8】

従って、これらの業種等では、日常的に通信量も多いことが想定できるため、その平均的な受信件数を考慮して所定値（件数等）を設定すればよい。

【0 0 6 9】

また、このようなアクセスが殺到した場合であっても、(D)DoS 攻撃に相当するような全く同じ時間（瞬間的）に大量の情報が送信されてくることは想定されるが、判定のための

一定時間の設定を短くするといった設定変更でも対応は可能である。

【0 0 7 0】

また、不正攻撃元探索もできる。

【0 0 7 1】

また、特定のサーバが近隣にない、ネットワークの中間点であっても判定された不正攻撃先を割りだすことができる。（請求項 9）

【図面の簡単な説明】

【0 0 7 2】

【図 1】 本発明の (D) DoS 攻撃検知およびその追跡システムの概念図である。

【図 2】 (A) はパケットデータフォーマットの説明図、(B) は通信量の一例を時系列で示したグラフ図、(C) はパケットのアドレス件数の一例を時系列で示したグラフ図である。

【図 3】 パケット探索を示す概念図である。

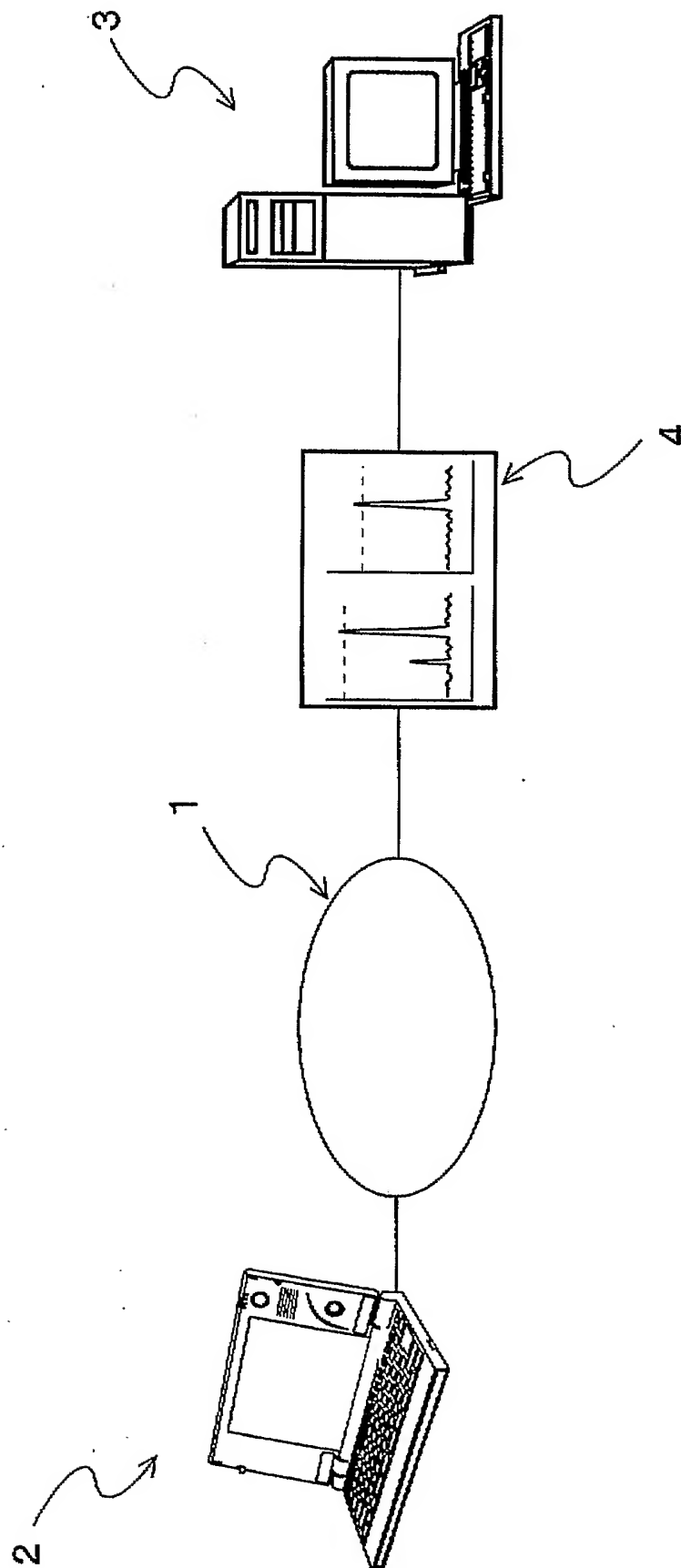
【図 4】 インターネットのシステムを示す概念図である。

【符号の説明】

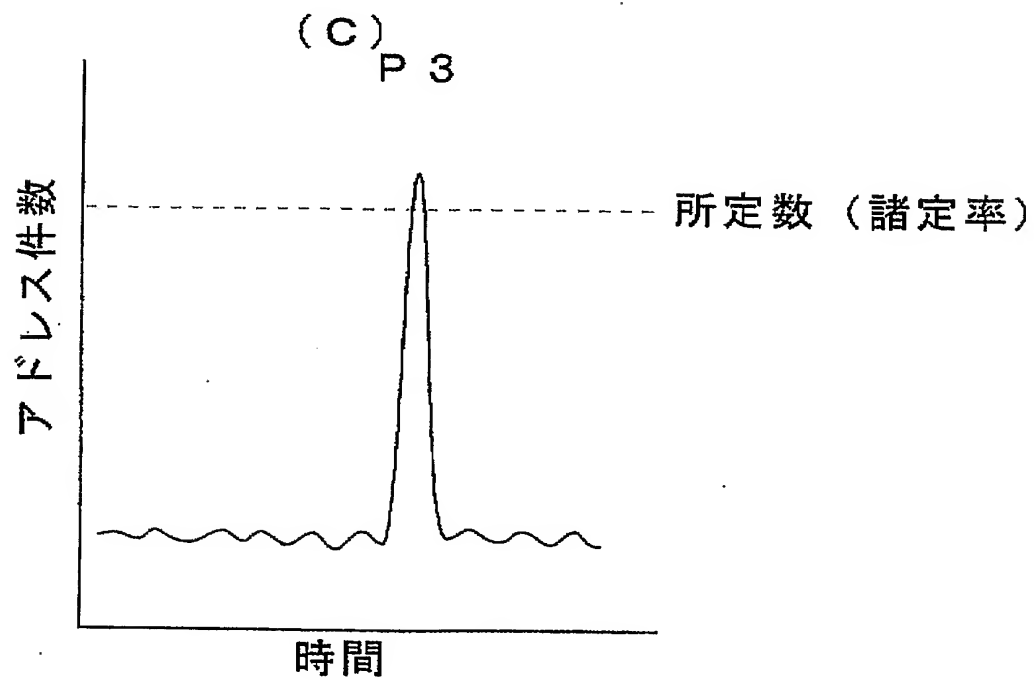
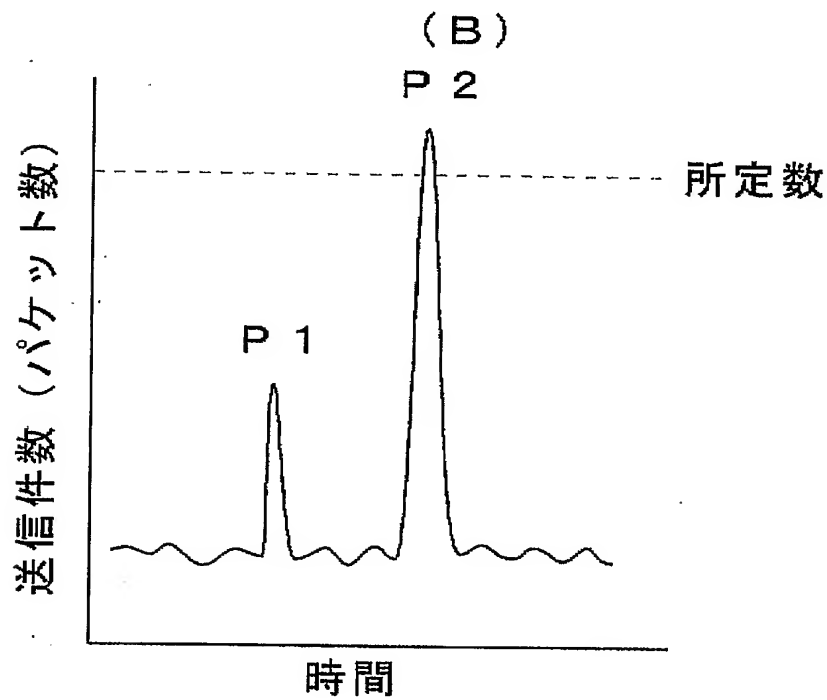
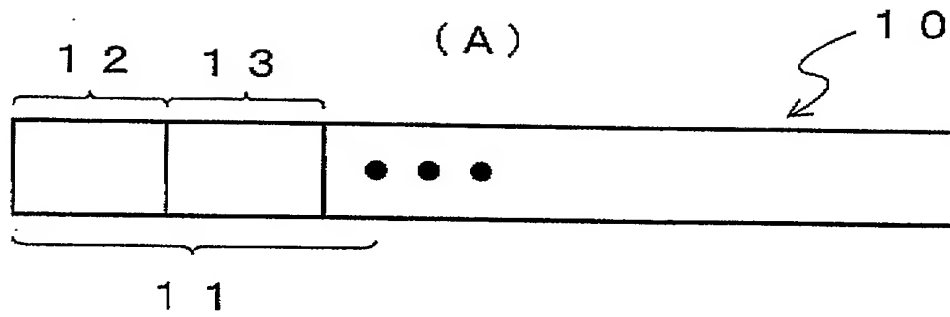
【0 0 7 3】

- 1 … インターネット回線
- 2 … 送信側コンピュータ
- 3 … 受信側コンピュータ
- 4 … 通信監視装置（判定手段）

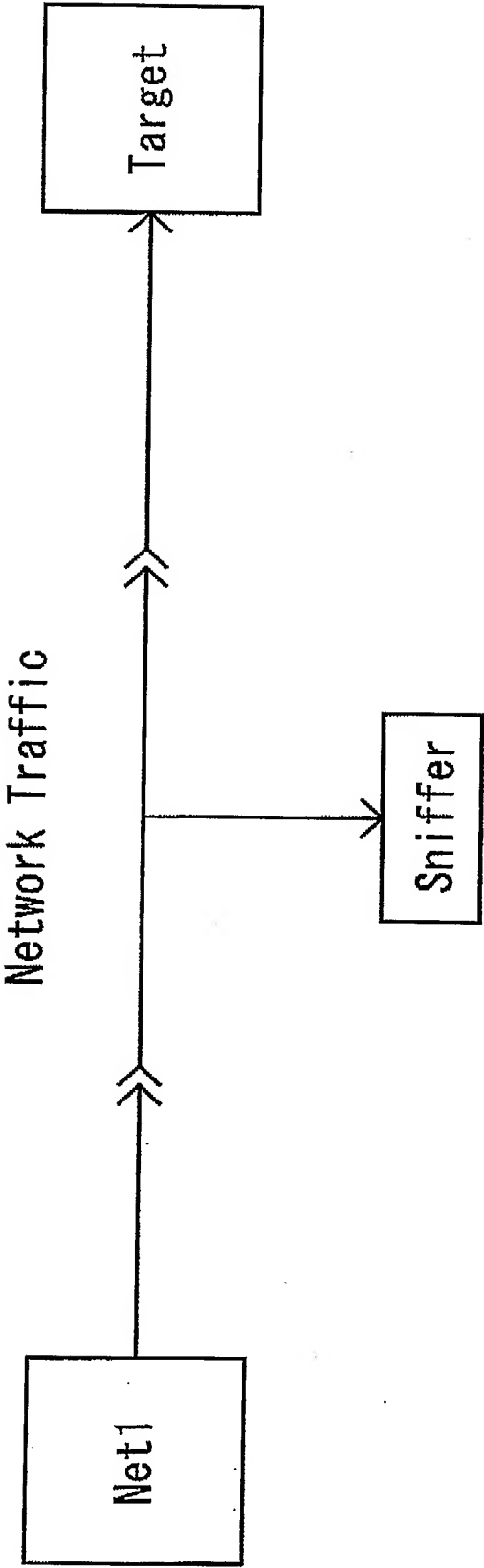
【書類名】 図面
【図 1】



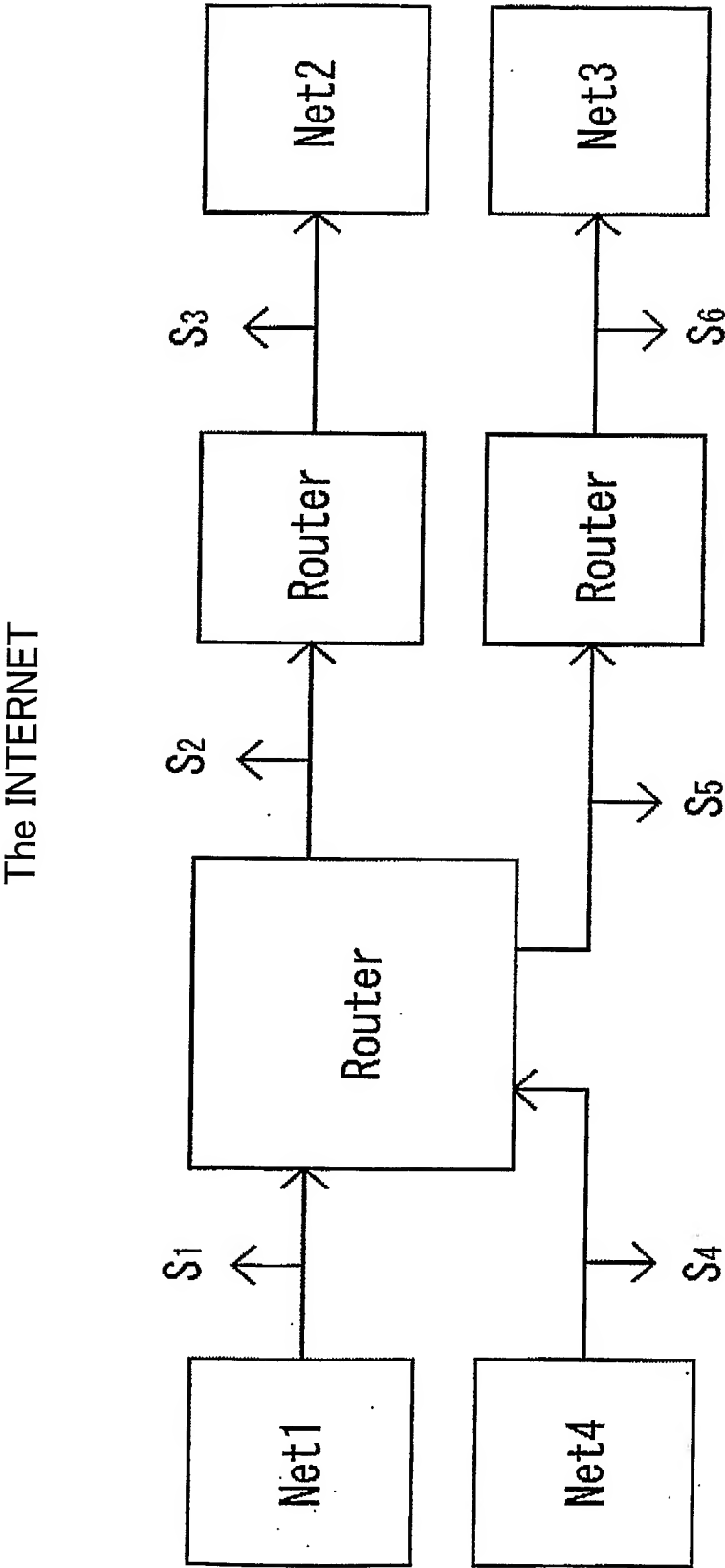
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 (D)DoS攻撃であるか否かの判定基準を容易化することができる (D)DoS攻撃検知および追跡、攻撃先特定システムを提供すること。

【解決手段】 インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フィールドの値の数が一定時間内で所定数、若しくは所定率に達した場合には不正攻撃が行われていると判定することを特徴とする。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 4 - 3 0 7 9 5 3
受付番号	5 0 4 0 1 8 0 4 9 6 3
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 6 年 1 0 月 2 7 日

<認定情報・付加情報>

【提出日】 平成16年10月22日

特願 2 0 0 4 - 3 0 7 9 5 3

ページ： 1/E

出 願 人 履 歴 情 報

識別番号

[5 0 1 1 7 5 2 8 1]

1. 変更年月日

2 0 0 1 年 4 月 2 7 日

[変更理由]

新規登録

住 所

宮城県仙台市青葉区南吉成六丁目 6 番地の 3

氏 名

株式会社サイバー・ソリューションズ